ABSTRACT

[1073] Techniques for associating software with hardware using cryptography are described. The software is identified by a software identifier (ID), and the hardware is identified by a hardware ID. The software is hashed to obtain a code digest. A code signature is generated for the code digest, software ID, and hardware ID. A code image is formed with the software, software ID, code signature, and a certificate. The certificate contains cryptographic information used to authenticate the certificate and validate the code signature. The code image is loaded onto a device. The device validates the software to hardware association prior to executing the software. For the validation, the device authenticates the certificate with a certificate authority public key embedded within the device. The device also validates the code signature using the cryptographic information contained in the certificate, information in the code image, and the hardware ID embedded within the device.